PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069597
(43)Date of publication of application : 07.03.2003

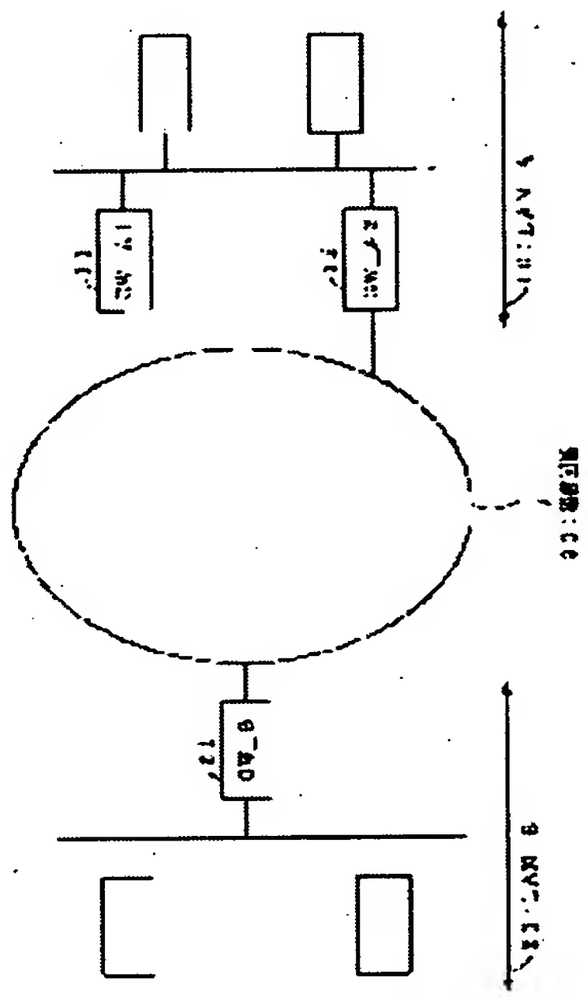
(51)Int.CI. H04L 12/46
H04L 9/08
H04L 12/66

(21)Application number : 2001-257681
(22)Date of filing : 28.08.2001

(71)Applicant : NEC CORP
(72)Inventor : YAMAGUCHI TAKAHIRO

(54) LARGE-SCALE IPSec VPN CONSTRUCTION METHOD, LARGE-SCALE IPSec VPN SYSTEM AND PROGRAM, AND KEY SHARING INFORMATION PROCESSING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To enable IPSec (Security architecture for IP) communication using a key even if a fault occurs in a gateway where a key exchange is performed, in a large-scale LAN having a plurality of gateways.
SOLUTION: When the key exchange based on IPSec is performed between the gateway of the large-scale LAN having a plurality of gateways and a gateway of another LAN, an Internet key exchange portion in the gateway of the large-scale LAN sets a key in an IPSec portion of this gateway, and requests a key transferring portion of this gateway to transfer the key. In response to this request, the key transferring portion transfers the key to a key transferring portion of another gateway in the large-scale LAN, and the key transferring portion of the other gateway sets the key in an IPSec portion of the other gateway by using this transferred key.



LEGAL STATUS
[Date of request for examination] 19.07.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3651424
[Date of registration] 04.03.2005
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（A）　(11)特許出願公開番号
特開2003－69597
(P2003－69597A)
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
H04L 12/46		H04L 12/46	V　5J104
	100		100R　5K030
9/08		12/66	B　5K033
12/66		9/00	601C
			601E

審査請求　有　請求項の数13　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－257681(P2001－257681)

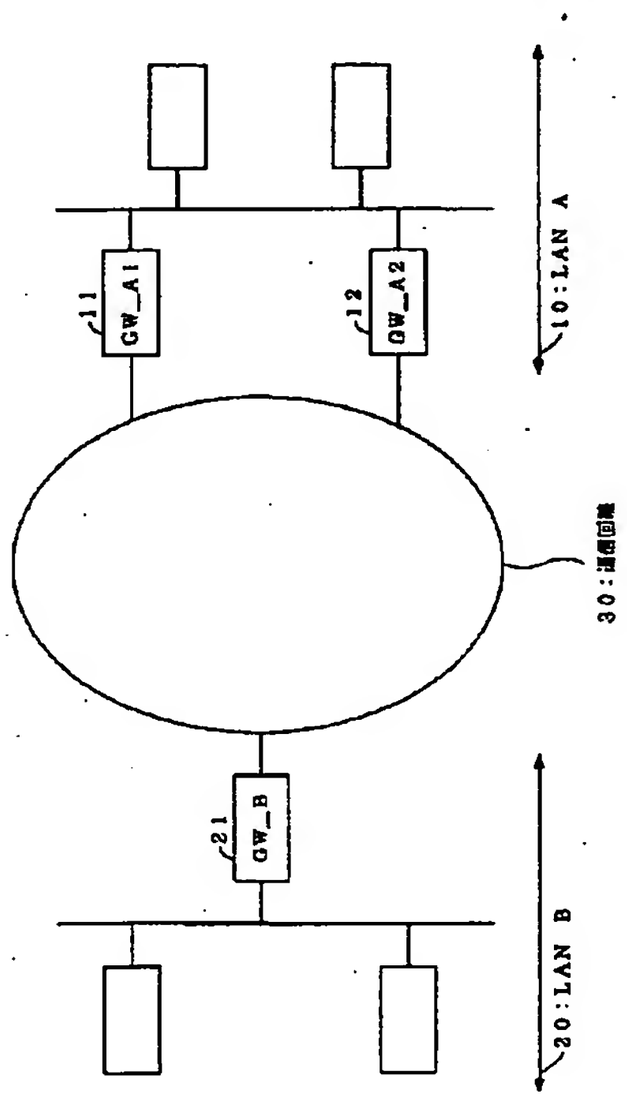
(22)出願日　平成13年８月28日(2001.8.28)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　山口　恭弘
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100086759
弁理士　渡辺　喜平

Ｆターム(参考)　5J104 AA16 EA02 EA04 EA16 JA03
NA02 PA07
5K030 GA11 HA08 HC14 HD03 LD19
5K033 AA04 CB01 CC01 DA01 DA05
DB19 EA03

(54)【発明の名称】　大規模ＩＰＳｅｃＶＰＮ構築方法、大規模ＩＰＳｅｃＶＰＮシステム、プログラム及び鍵共有情報処理装置

(57)【要約】
【課題】　複数のゲートウェイを有する大規模ＬＡＮにおいて、鍵交換を行ったゲートウェイに障害が発生しても、その鍵を使ったＩＰＳｅｃ通信を可能とする。
【解決手段】　複数のゲートウェイを有する大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイとの間で、ＩＰＳｅｃにもとづく鍵交換が行われた場合において、大規模ＬＡＮのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、この要求に応じて鍵転送部が、大規模ＬＡＮの他のゲートウェイの鍵転送部に鍵転送を行い、他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、他のゲートウェイのＩＰＳｅｃ部に鍵設定を行う。



【特許請求の範囲】

【請求項１】　複数のゲートウェイを有する大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイとの間で、ＩＰＳｅｃにもとづく鍵交換が行われた場合において、

前記大規模ＬＡＮのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、

前記ゲートウェイの鍵転送部が、前記要求に応じて、前記大規模ＬＡＮの他のゲートウェイの鍵転送部に鍵転送を行い、

前記他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、前記他のゲートウェイのＩＰＳｅｃ部に鍵設定を行うことを特徴とする大規模ＩＰＳｅｃ　ＶＰＮの構築方法。

【請求項２】　前記鍵転送は、

前記大規模ＬＡＮの前記ゲートウェイが、前記大規模ＬＡＮの前記他のゲートウェイに鍵転送を要求し、

前記他のゲートウェイが、この要求に対して、ＯＫ信号を暗号化して前記ゲートウェイに返し、

前記ゲートウェイが、この暗号化されたＯＫ信号を検査するとともに、前記鍵を暗号化して前記他のゲートウェイに転送し、

前記他のゲートウェイが、この転送されてきた鍵を検査して、前記ゲートウェイにＯＫ信号を返す手順を含むことを特徴とする請求項１記載の大規模ＩＰＳｅｃ　ＶＰＮの構築方法。

【請求項３】　前記大規模ＬＡＮの前記他のゲートウェイの鍵転送部が、前記大規模ＬＡＮの前記ゲートウェイから鍵転送を受けると、前記他のゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を前記大規模ＬＡＮのさらなる他のゲートウェイの鍵転送部に転送し、

前記さらなる他のゲートウェイも、前記他のゲートウェイと同様に、自分のＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を前記ゲートウェイの鍵転送部に転送し、

前記ゲートウェイは、転送されてきた前記鍵が、最初に自分が転送した鍵に一致すること確認することを特徴とする請求項１又は２記載の大規模ＩＰＳｅｃ　ＶＰＮの構築方法。

【請求項４】　複数のゲートウェイを有する大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイとの間で、ＩＰＳｅｃにもとづく鍵交換が行われると、前記大規模ＬＡＮ内のゲートウェイ間で鍵転送が行われる大規模ＩＰＳｅｃ　ＶＰＮシステムであって、

インターネットキーエクスチェンジ部により前記その他のＬＡＮのゲートウェイと鍵交換を行うとともに、このインターネットキーエクスチェンジ部により自分のＩＰＳｅｃ部に鍵設定を行って、自分の鍵転送部に鍵転送を要求し、この鍵転送部により前記大規模ＬＡＮの他のゲートウェイに鍵転送を行う前記大規模ＬＡＮの前記ゲートウェイと、

前記大規模ＬＡＮの前記ゲートウェイから、鍵転送部が鍵転送を受けるとともに、自分のＩＰＳｅｃ部に鍵設定を行う前記大規模ＬＡＮの前記他のゲートウェイと、

前記大規模ＬＡＮの前記ゲートウェイと鍵交換を行う前記その他のＬＡＮのゲートウェイと、

前記大規模ＬＡＮの前記ゲートウェイと、前記大規模ＬＡＮの前記他のゲートウェイと、前記その他のＬＡＮのゲートウェイを接続する通信回線とを有することを特徴とする大規模ＩＰＳｅｃ　ＶＰＮシステム。

【請求項５】　前記鍵転送は、

前記大規模ＬＡＮの前記ゲートウェイが、前記大規模ＬＡＮの前記他のゲートウェイに鍵転送を要求し、

前記他のゲートウェイが、この要求に対して、ＯＫ信号を暗号化して前記ゲートウェイに返し、

前記ゲートウェイが、この暗号化されたＯＫ信号を検査するとともに、前記鍵を暗号化して前記他のゲートウェイに転送し、

前記他のゲートウェイが、この転送されてきた鍵を検査して、前記ゲートウェイにＯＫ信号を返す手順を含むことを特徴とする請求項４記載の大規模ＩＰＳｅｃ　ＶＰＮシステム。

【請求項６】　前記大規模ＬＡＮの前記他のゲートウェイの鍵転送部が、前記大規模ＬＡＮの前記ゲートウェイから鍵転送を受けると、前記他のゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を前記大規模ＬＡＮのさらなる他のゲートウェイの鍵転送部に転送し、

前記さらなる他のゲートウェイも、前記他のゲートウェイと同様に、自分のＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を前記ゲートウェイの鍵転送部に転送し、

前記ゲートウェイは、転送されてきた前記鍵が、最初に自分が転送した鍵に一致すること確認することを特徴とする請求項４又は５記載の大規模ＩＰＳｅｃ　ＶＰＮシステム。

【請求項７】　前記転送が、前記大規模ＬＡＮが有する４台以上のゲートウェイについて同様に行われることを特徴とする請求項６記載の大規模ＩＰＳｅｃ　ＶＰＮシステム。

【請求項８】　前記大規模ＬＡＮの前記ゲートウェイと、前記その他のＬＡＮのゲートウェイが鍵交換を行うとともに、前記大規模ＬＡＮの前記ゲートウェイが、前記大規模ＬＡＮの前記他のゲートウェイに鍵転送を行い、

前記大規模ＬＡＮの前記ゲートウェイに障害が発生すると、

通信回線上の複数のルータの情報交換によって、前記大規模ＬＡＮの前記ゲートウェイ宛の転送を、前記大規模ＬＡＮの前記他のゲートウェイに対して行うように経路情報が修正され、

前記大規模ＬＡＮのホストに対して、前記その他のＬＡＮの他のホストからパケット発信がなされると、前記その他のＬＡＮのゲートウェイが、このパケットをカプセル化して、前記大規模ＬＡＮの前記ゲートウェイ宛に通信回線を介して送信し、
前記送信されたパケットが、前記修正された経路情報に従って、前記大規模ＬＡＮの前記他のゲートウェイに転送され、
前記大規模ＬＡＮの前記他のゲートウェイが、前記送信されたパケットの逆カプセル化を行って、前記大規模ＬＡＮの前記ホストに送信し、
前記大規模ＬＡＮの前記ホストがこの送信されてきたパケットの受信を行うことを特徴とする請求項４～７のいずれかに記載の大規模ＩＰＳｅｃ　ＶＰＮシステム。
【請求項９】　大規模ＬＡＮ内において、鍵転送を行う大規模ＩＰＳｅｃＶＰＮプログラムであって、
前記大規模ＬＡＮのゲートウェイのインターネットキーエクスチェンジ部が、鍵交換を行った場合には、前記ゲートウェイのインターネットキーエクスチェンジ部に、前記ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせるとともに、前記ゲートウェイの鍵転送部に対して鍵転送を要求させ、
前記ゲートウェイの鍵転送部に、前記大規模ＬＡＮの他のゲートウェイの鍵転送部に対して鍵転送を行わせ、
前記大規模ＬＡＮの前記ゲートウェイの鍵転送部が、鍵転送を受けた場合には、この鍵転送部に、転送されてきた鍵を用いて、前記ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせることを実行させるための大規模ＩＰＳｅｃ　ＶＰＮプログラム。
【請求項１０】　前記鍵転送は、
前記大規模ＬＡＮの前記ゲートウェイに、前記大規模ＬＡＮの前記他のゲートウェイに対して鍵転送を要求させ、
前記他のゲートウェイに、この要求に対して、ＯＫ信号を暗号化させて前記ゲートウェイに返却させ、
前記ゲートウェイに、この暗号化されたＯＫ信号を検査させるとともに、前記鍵を暗号化させて前記他のゲートウェイに転送させ、
前記他のゲートウェイに、この転送されてきた鍵を検査させて、前記ゲートウェイにＯＫ信号を返却させる手順を含むことを特徴とする請求項９記載の大規模ＩＰＳｅｃ　ＶＰＮプログラム。
【請求項１１】　前記大規模ＬＡＮの前記ゲートウェイの鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、前記ゲートウェイの鍵転送部に、前記ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせるとともに、前記大規模ＬＡＮのさらなる他のゲートウェイに対して鍵転送を行わせることを特徴とする請求項９又は１０記載の大規模ＩＰＳｅｃ　ＶＰＮプログラム。

【請求項１２】　通信回線を介してＩＰＳｅｃによる鍵交換を行う際に、鍵転送も行う鍵共有情報処理装置であって、
前記鍵共有情報処理装置のインターネットキーエクスチェンジ部が、鍵交換を行った場合には、このインターネットキーエクスチェンジ部が、前記鍵共有情報処理装置のＩＰＳｅｃ部に鍵設定を行うとともに、前記鍵共有情報処理装置の鍵転送部に鍵転送を要求し、この鍵転送部が他の鍵共有情報処理装置に鍵転送を行い、
前記鍵共有情報処理装置の鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、前記鍵共有情報処理装置のＩＰＳｅｃ部に鍵設定を行うことを特徴とする鍵共有情報処理装置。
【請求項１３】　前記鍵共有情報処理装置が、大規模ＩＰＳｅｃ　ＶＰＮにおけるゲートウェイであることを特徴とする請求項１２記載の鍵共有情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数のゲートウェイを有する大規模ＬＡＮとＩＰＳｅｃによるＶＰＮを構築するにあたり、鍵交換とともに鍵転送を行うことによって、一部のゲートウェイに障害が発生しても、通信不能とならない大規模ＩＰＳｅｃ　ＶＰＮ構築方法、大規模ＩＰＳｅｃ　ＶＰＮシステム、大規模ＩＰＳｅｃ　ＶＰＮプログラム及び鍵共有情報処理装置に関する。
【０００２】
【従来の技術】ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ　ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ））は特定のメンバ間で秘密鍵を共有することによってセキュリティを確保している。この秘密鍵を共有するためには、通常ＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ；インターネットキーエクスチェンジ）プロトコルを用いるが、これは特定の２者間で秘密鍵を生成するプロトコルであるため、事実上ＩＰＳｅｃは、特定２者間でセキュリティを確保するプロトコルになっている。
【０００３】一方、大企業のネットワークなどの大規模なＬＡＮは、通常ＬＡＮ外からの通信を受け入れるために、複数のゲートウェイを持っている。そのため、一つのゲートウェイで障害が発生しても別のゲートウェイを経由して、ＬＡＮ外からの通信が可能になる。
【０００４】ところが、ＩＰＳｅｃを用いると、ＬＡＮ外の装置は一つのゲートウェイとの間でしかセキュリティを確保できなくなるため、このゲートウェイにおいて障害が発生するとＬＡＮ内との通信ができなくなってしまっていた。このような問題を解決するために、ＩＰＳｅｃによるセキュリティの確保が行われたゲートウェイに障害が発生した場合には、その時点で別のゲートウェイとの間で新たにＩＰＳｅｃ通信を行う方法なども行われている。

【０００５】
【発明が解決しようとする課題】しかしながら、このような従来の方法などは、ゲートウェイの障害に備えて、常にその動作状況を監視する必要があることに加え、障害が発生した場合には、別のゲートウェイと再度新たに鍵の共有を行う必要があり、ネットワークに高い負荷をかける方法であった。このため、一つのゲートウェイで障害が発生しても別のゲートウェイを経由してＬＡＮ外との通信を行うことのできる大規模ＬＡＮの利点を損なうことなく、ＩＰＳｅｃによるセキュリティの確保を可能とする方法等の実現が望まれていた。
【０００６】本発明は、上記の事情にかんがみなされたものであり、従来のようなＩＰＳｅｃにおける不都合を解消し、ＩＰＳｅｃによるセキュリティの確保されたゲートウェイにおいて障害が発生しても、ネットワークに高負荷をかけることなく、別のゲートウェイを経由して、ＬＡＮ外からの通信を可能とする大規模ＩＰＳｅｃ　ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）構築方法、大規模ＩＰＳｅｃ　ＶＰＮシステム、大規模ＩＰＳｅｃ　ＶＰＮプログラム及び鍵共有情報処理装置の提供を目的とする。
【０００７】
【課題を解決するための手段】上記目的を達成するため、本発明の請求項１記載の大規模ＩＰＳｅｃ　ＶＰＮの構築方法は、複数のゲートウェイを有する大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイとの間で、ＩＰＳｅｃにもとづく鍵交換が行われた場合において、大規模ＬＡＮのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、ゲートウェイの鍵転送部が、要求に応じて、大規模ＬＡＮの他のゲートウェイの鍵転送部に鍵転送を行い、他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、他のゲートウェイのＩＰＳｅｃ部に鍵設定を行う方法としてある。
【０００８】大規模ＩＰＳｅｃ　ＶＰＮの構築方法をこのような方法にすれば、大規模ＬＡＮ内において、鍵交換を行ったゲートウェイが、他のゲートウェイにその鍵をコピーし、実際には鍵交換を行っていないゲートウェイに、鍵交換行った場合と同様の権限をもたせることができる。
【０００９】このため、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイが、その障害が発生したゲートウェイに代わり、同様の役割を果たすことが可能となるため、このような場合に通信不能とはならなくなる。また、この方法によれば、余分に鍵交換を行う必要がなくなるため、ネットワークや、ゲートウェイにかかる負荷を大幅に軽減することが可能となる。
【００１０】次に、本発明の請求項２記載の大規模ＩＰＳｅｃ　ＶＰＮの構築方法は、鍵転送は、大規模ＬＡＮ

のゲートウェイが、大規模ＬＡＮの他のゲートウェイに鍵転送を要求し、他のゲートウェイが、この要求に対して、ＯＫ信号を暗号化してゲートウェイに返し、ゲートウェイが、この暗号化されたＯＫ信号を検査するとともに、鍵を暗号化して他のゲートウェイに転送し、他のゲートウェイが、この転送されてきた鍵を検査して、ゲートウェイにＯＫ信号を返す手順を含む方法としてある。
【００１１】大規模ＩＰＳｅｃ　ＶＰＮの構築方法をこのような方法にすれば、鍵転送を行う場合において、セキュリティを確保することが可能となり、この鍵転送を行うＬＡＮの内部に悪意のユーザが存在したとしても、盗聴などが行われることを防止することができる。
【００１２】次に、本発明の請求項３記載の大規模ＩＰＳｅｃ　ＶＰＮの構築方法は、大規模ＬＡＮの他のゲートウェイの鍵転送部が、大規模ＬＡＮのゲートウェイから鍵転送を受けると、他のゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を大規模ＬＡＮのさらなる他のゲートウェイの鍵転送部に転送し、さらなる他のゲートウェイも、他のゲートウェイと同様に、自分のＩＰＳｅｃ部に鍵設定を行うとともに、この鍵をゲートウェイの鍵転送部に転送し、ゲートウェイは、転送されてきた鍵が、最初に自分が転送した鍵に一致すること確認する方法としてある。
【００１３】大規模ＩＰＳｅｃ　ＶＰＮの構築方法をこのような方法にすれば、大規模ＬＡＮのゲートウェイが、３台以上の場合には、鍵転送を受けたゲートウェイが、さらに他のゲートウェイに鍵転送を行うことができ、鍵転送を効率的に行うことが可能となる。また、大規模ＬＡＮ内のゲートウェイが多数ある場合には、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、同時に複数の転送を行うことによって、速やかに鍵転送を行うことも可能となる。
【００１４】次に、本発明の請求項４記載の大規模ＩＰＳｅｃ　ＶＰＮシステムは、複数のゲートウェイを有する大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイとの間で、ＩＰＳｅｃにもとづく鍵交換が行われると、大規模ＬＡＮ内のゲートウェイ間で鍵転送が行われる大規模ＩＰＳｅｃ　ＶＰＮシステムであって、インターネットキーエクスチェンジ部によりその他のＬＡＮのゲートウェイと鍵交換を行うとともに、このインターネットキーエクスチェンジ部により自分のＩＰＳｅｃ部に鍵設定を行って、自分の鍵転送部に鍵転送を要求し、この鍵転送部により大規模ＬＡＮの他のゲートウェイに鍵転送を行う大規模ＬＡＮのゲートウェイと、大規模ＬＡＮのゲートウェイから、鍵転送部が鍵転送を受けるとともに、自分のＩＰＳｅｃ部に鍵設定を行う大規模ＬＡＮの他のゲートウェイと、大規模ＬＡＮのゲートウェイと鍵交換を行うその他のＬＡＮのゲートウェイと、大規模ＬＡＮのゲートウェイと、大規模ＬＡＮの他のゲートウェイと、その他のＬＡＮのゲートウェイを接続す

る通信回線とを有する構成としてある。

【００１５】大規模ＩＰＳｅｃ　ＶＰＮシステムをこのような構成にすれば、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイが、その障害が発生したゲートウェイに代わり、同様の役割を果たすことが可能となるため、ＩＰＳｅｃ通信不能とはならなくなる。

【００１６】また、従来技術にあるように、別途鍵交換を行うことによって、迂回用のゲートウェイを設定する場合に比べると、本システムでは負荷の大きい鍵交換を１度しか行う必要がないため、ネットワークや、ゲートウェイにかかる負荷を大幅に軽減することが可能となる。

【００１７】次に、本発明の請求項５記載の大規模ＩＰＳｅｃ　ＶＰＮシステムは、鍵転送は、大規模ＬＡＮのゲートウェイが、大規模ＬＡＮの他のゲートウェイに鍵転送を要求し、他のゲートウェイが、この要求に対して、ＯＫ信号を暗号化してゲートウェイに返し、ゲートウェイが、この暗号化されたＯＫ信号を検査するとともに、鍵を暗号化して他のゲートウェイに転送し、他のゲートウェイが、この転送されてきた鍵を検査して、ゲートウェイにＯＫ信号を返す手順を含む構成としてある。

【００１８】大規模ＩＰＳｅｃ　ＶＰＮシステムをこのような構成にすれば、ＬＡＮの内部に悪意のユーザが存在したとしても、鍵転送時における盗聴などを防止することが可能となる。

【００１９】次に、本発明の請求項６記載の大規模ＩＰＳｅｃ　ＶＰＮシステムは、大規模ＬＡＮの他のゲートウェイの鍵転送部が、大規模ＬＡＮのゲートウェイから鍵転送を受けると、他のゲートウェイのＩＰＳｅｃ部に鍵設定を行うとともに、この鍵を大規模ＬＡＮのさらなる他のゲートウェイの鍵転送部に転送し、さらなる他のゲートウェイも、他のゲートウェイと同様に、自分のＩＰＳｅｃ部に鍵設定を行うとともに、この鍵をゲートウェイの鍵転送部に転送し、ゲートウェイは、転送されてきた鍵が、最初に自分が転送した鍵に一致すること確認する構成としてある。

【００２０】大規模ＩＰＳｅｃ　ＶＰＮシステムをこのような構成にすれば、大規模ＬＡＮのゲートウェイが、３台以上の場合には、鍵転送を受けたゲートウェイが、さらに他のゲートウェイに鍵転送を行うことができ、鍵転送を効率的に行うことが可能となる。

【００２１】次に、本発明の請求項７記載の大規模ＩＰＳｅｃ　ＶＰＮシステムは、転送が、大規模ＬＡＮが有する４台以上のゲートウェイについて同様に行われる構成としてある。この転送とは、請求項６における鍵設定、鍵転送及び鍵の確認を含む鍵を転送する際の一連の処理を意味する。大規模ＩＰＳｅｃ　ＶＰＮシステムをこのような構成にすれば、大規模ＬＡＮが多数のゲートウェイを有する場合であっても、鍵転送を受けたゲートウェイ自体も、他のゲートウェイに対して鍵転送を行うことが可能となる。

【００２２】この場合、鍵転送を受けたゲートウェイが、次に他のゲートウェイに鍵転送を順次行うといったように、単に複数の鍵転送を直線的に実施するのみならず、所定の鍵転送経路を設定するなどして、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、複数の転送を同時に実行することによって、速やかに転送を行うことも可能である。

【００２３】次に、本発明の請求項８記載の大規模ＩＰＳｅｃ　ＶＰＮシステムは、大規模ＬＡＮのゲートウェイと、その他のＬＡＮのゲートウェイが鍵交換を行うとともに、大規模ＬＡＮのゲートウェイが、大規模ＬＡＮの他のゲートウェイに鍵転送を行い、大規模ＬＡＮのゲートウェイに障害が発生すると、通信回線上の複数のルータの情報交換によって、大規模ＬＡＮのゲートウェイ宛の転送を、大規模ＬＡＮの他のゲートウェイに対して行うように経路情報が修正され、大規模ＬＡＮのホストに対して、その他のＬＡＮの他のホストからパケット発信がなされると、その他のＬＡＮのゲートウェイが、このパケットをカプセル化して、大規模ＬＡＮのゲートウェイ宛に通信回線を介して送信し、送信されたパケットが、修正された経路情報に従って、大規模ＬＡＮの他のゲートウェイに転送され、大規模ＬＡＮの他のゲートウェイが、送信されたパケットの逆カプセル化を行って、大規模ＬＡＮのホストに送信し、大規模ＬＡＮのホストがこの送信されてきたパケットの受信を行う構成としてある。

【００２４】大規模ＩＰＳｅｃ　ＶＰＮシステムをこのような構成にすれば、大規模ＬＡＮにおける鍵交換を行ったゲートウェイに障害が発生しても、鍵交換を行った時点で事前に、大規模ＬＡＮにおける他のゲートウェイに鍵転送が行われているため、その他のＬＡＮの他のホストから、その他のＬＡＮにおける上記鍵交換を行ったゲートウェイを経由して、大規模ＬＡＮのホストに対してパケットが送信された場合に、上記障害が発生したゲートウェイを迂回し、鍵転送を受けた他のゲートウェイを経由して、適切なホストに受信させることが可能となる。なお、この場合のホストとは、所謂ホストコンピュータに限定する意味のものではなく、端末やサーバ等、ネットワークに接続する広く一般の情報処理装置を意味するものである。

【００２５】次に、本発明の請求項９記載の大規模ＩＰＳｅｃ　ＶＰＮプログラムは、大規模ＬＡＮ内において、鍵転送を行う大規模ＩＰＳｅｃ　ＶＰＮプログラムであって、大規模ＬＡＮのゲートウェイのインターネットキーエクスチェンジ部が、鍵交換を行った場合には、ゲートウェイのインターネットキーエクスチェンジ部に、ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせるとともに、ゲートウェイの鍵転送部に対して鍵転送

を要求させ、ゲートウェイの鍵転送部に、大規模ＬＡＮの他のゲートウェイの鍵転送部に対して鍵転送を行わせ、大規模ＬＡＮのゲートウェイの鍵転送部が、鍵転送を受けた場合には、この鍵転送部に、転送されてきた鍵を用いて、ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせる構成としてある。

【００２６】大規模ＩＰＳｅｃ　ＶＰＮプログラムをこのような構成にすれば、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイにその代役をさせることができるため、このような場合にＩＰＳｅｃ通信不能となることを防止することが可能となる。また、従来技術の別途鍵交換を行うことにより迂回用のゲートウェイを設定する場合に比べると、負荷の大きい鍵交換を１度しか行わせないため、ネットワークや、ゲートウェイにかかる負荷を大幅に軽減させることが可能となる。

【００２７】次に、本発明の請求項１０記載の大規模ＩＰＳｅｃ　ＶＰＮプログラムは、鍵転送は、大規模ＬＡＮのゲートウェイに、大規模ＬＡＮの他のゲートウェイに対して鍵転送を要求させ、他のゲートウェイに、この要求に対して、ＯＫ信号を暗号化させてゲートウェイに返却させ、ゲートウェイに、この暗号化されたＯＫ信号を検査させるとともに、鍵を暗号化させて他のゲートウェイに転送させ、他のゲートウェイに、この転送されてきた鍵を検査させて、ゲートウェイにＯＫ信号を返却させる手順を含む構成としてある。

【００２８】大規模ＩＰＳｅｃ　ＶＰＮプログラムをこのような構成にすれば、ＬＡＮの内部に悪意のユーザが存在したとしても、鍵転送時における盗聴などを防止させることが可能となる。

【００２９】次に、本発明の請求項１１記載の大規模ＩＰＳｅｃ　ＶＰＮプログラムは、大規模ＬＡＮのゲートウェイの鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、ゲートウェイの鍵転送部に、ゲートウェイのＩＰＳｅｃ部に対して鍵設定を行わせるとともに、大規模ＬＡＮのさらなる他のゲートウェイに対して鍵転送を行わせる構成としてある。

【００３０】大規模ＩＰＳｅｃ　ＶＰＮプログラムをこのような構成にすれば、大規模ＬＡＮのゲートウェイが、３台以上の場合に、鍵転送を受けたゲートウェイに、さらに他のゲートウェイへ鍵転送を行わせることができるため、鍵転送の効率化を図ることが可能となる。

【００３１】次に、本発明の請求項１２記載の鍵共有情報処理装置は、通信回線を介してＩＰＳｅｃによる鍵交換を行う際に、鍵転送も行う鍵共有情報処理装置であって、鍵共有情報処理装置のインターネットキーエクスチェンジ部が、鍵交換を行った場合には、このインターネットキーエクスチェンジ部が、鍵共有情報処理装置のＩＰＳｅｃ部に鍵設定を行うとともに、鍵共有情報処理装置の鍵転送部に鍵転送を要求し、この鍵転送部が他の鍵共有情報処理装置に鍵転送を行い、鍵共有情報処理装置

の鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、鍵共有情報処理装置のＩＰＳｅｃ部に鍵設定を行う構成としてある。

【００３２】鍵共有情報処理装置をこのような構成にすれば、自分が鍵交換を行った場合には、自身のＩＰＳｅｃ部に鍵設定を行うとともに、他の鍵共有情報処理装置に鍵を転送し、他の鍵共有情報処理装置が鍵設定を行った場合には、鍵転送を受けるとともに、この転送されてきた鍵を自身のＩＰＳｅｃ部に設定することが可能となる。

【００３３】そして、大規模ＬＡＮなどにおいて、このような鍵共有情報処理装置をＬＡＮ外との情報の送受信の窓口として用いることにより、特定の鍵共有情報処理装置に障害が発生しても、この鍵共有情報処理装置から鍵転送を受けた他の鍵共有情報処理装置が、その代役を果たすことにより、通信不能となることを防止することが可能となる。

【００３４】また、このような鍵共有情報処理装置を、大規模ＩＰＳｅｃ　ＶＰＮ以外に応用してもかまわない。例えば、インターネットショッピングなどにおいて、利用者端末が、ショップにおける本発明の鍵共有情報処理装置とセキュリティを確立する際に、ショップの別個の鍵共有情報処理装置に鍵転送を行うことによって、利用者のショッピング中にショップの鍵共有情報処理装置に障害が発生しても、その別個の鍵共有情報処理装置に以降の処理を代行させることによって、通信不能となることを防止することが可能となる。

【００３５】次に、本発明の請求項１３記載の鍵共有情報処理装置は、大規模ＩＰＳｅｃＶＰＮにおけるゲートウェイである構成としてある。鍵共有情報処理装置をこのような構成にすれば、上記のような鍵転送機能を大規模ＩＰＳｅｃ　ＶＰＮにおけるゲートウェイにもたせることが可能となる。

【００３６】

【発明の実施の形態】以下、本発明の実施形態につき、図面を参照して説明する。

［第一実施形態］まず、本発明の第一実施形態について、図１を参照して説明する。同図は、本実施形態における大規模ＩＰＳｅｃ．ＶＰＮシステムの構成を示すブロック図である。

【００３７】同図に示すように、大規模ＩＰＳｅｃ．ＶＰＮシステムは、ＬＡＮ　Ａ１０、ＬＡＮ　Ｂ２０及び通信回線３０を有している。ＬＡＮ　Ａ１０は、複数のゲートウェイを有する大規模ＬＡＮであって、ゲートウェイＡ１（ＧＷ＿Ａ１）１１とゲートウェイＡ２（ＧＷ＿Ａ２）１２等を有している。

【００３８】また、ＬＡＮ　Ｂ２０は、その他のＬＡＮであって、その規模に特に制限はないが、ゲートウェイＢ（ＧＷ＿Ｂ）２１等を有している。これらＬＡＮ　Ａ１０とＬＡＮ　Ｂ２０とは通信回線３０を介して接続さ

れている。

【００３９】そして、これらＬＡＮ　Ａ１０とＬＡＮ　Ｂ２０が通信するにあたり、ＩＰＳｅｃによるセキュリティを確保したい場合には、通常、例えばゲートウェイＡ１１１と、ゲートウェイＢ　２１が、ＩＫＥ（インターネットキーエクスチェンジ）による鍵交換を行って同じ鍵を共有し、その鍵を使ってＩＰＳｅｃ通信を行う。

【００４０】この際、本実施形態においては、ゲートウェイＡ１　１１と、ゲートウェイＢ２１が鍵交換を行うにあたり、ゲートウェイＡ１　１１が、ゲートウェイＡ２１２に鍵転送を行って、その後ゲートウェイＡ１　１１に障害が発生しても、ゲートウェイＡ２　１２にＩＰＳｅｃ通信機能を代行させることを可能とする。

【００４１】通信回線３０としては、従来公知の任意好適な公衆回線、商業回線又は専用回線を用いることができる。また、ゲートウェイＡ１　１１、ゲートウェイＡ２１２及びゲートウェイＢ　２１等のそれぞれの間においては、同一又は別個の通信回線で構成することができる。

【００４２】さらに、通信回線３０は、ゲートウェイＡ１　１１、ゲートウェイＡ２　１２及びゲートウェイＢ　２１等のそれぞれの間を、無線あるいは有線で接続可能な回線であり、例えば、携帯端末網、公衆回線網、専用回線網及びインターネット回線網により構成することができる。

【００４３】次に、図２を用いて、上記各ゲートウェイの機能について、その処理手順とともに詳細に説明する。ゲートウェイＡ１　１１は、ＩＫＥ部１１１、ＩＰＳｅｃ部１１２、鍵転送部１１３を有している。また、ゲートウェイＡ２　１２も同様に、ＩＫＥ部１２１、ＩＰＳｅｃ部１２２、鍵転送部１２３を有しており、ゲートウェイＢ　２１は、ＩＫＥ部２１１及びＩＰＳｅｃ部２１２を有している。

【００４４】そして、ＩＫＥ部１１１が、ＩＫＥ部２１１と鍵交換を行う（ステップ１０）と、これらはそれぞれ、ＩＰＳｅｃ部１１２、ＩＰＳｅｃ部２１２に鍵設定を行う（ステップ１１）。この鍵交換としては、ＩＫＥによる従来の鍵交換技術を用いる。そして、鍵設定によって、それぞれのＩＰＳｅｃ部に共通の鍵が設定される。

【００４５】次に、鍵交換を行ったゲートウェイＡ１１１のＩＫＥ部１１１は、鍵転送部１１３に鍵転送要求を行い（ステップ１２）、この鍵転送部１１３は、ゲートウェイＡ２　１２の鍵転送部１２３に鍵転送を行う（ステップ１３）。鍵転送を受けた鍵転送部１２３は、ＩＰＳｅｃ部１２２に鍵設定を行う（ステップ１４）。

【００４６】このようにすることによって、ゲートウェイＢ　２１のＩＰＳｅｃ部２１２は、ゲートウェイＡ１　１１のＩＰＳｅｃ部１１２とＩＰＳｅｃ通信を行うことができるとともに、ゲートウェイＡ１　１１に障害が発生して、これと通信を行うことができなくなった場合にあっても、ゲートウェイＡ２　１２のＩＰＳｅｃ部１２２とＩＰＳｅｃ通信を行うことが可能となる（ステップ１５）。

【００４７】次に、図３を用いて、上記鍵転送の処理手順について詳細に説明する。同図は、本実施形態の大規模ＩＰＳｅｃ　ＶＰＮシステムにおける鍵転送プロトコルの動作を表わす動作手順図である。まず、ゲートウェイＡ１　１１の鍵転送部１１３が、ゲートウェイＡ２　１２の鍵転送部１２３に対して、鍵転送を要求する（ステップ２０）。

【００４８】これに対して、鍵転送部１２３は、鍵転送部１１３にＯＫ信号を返す（ステップ２１）。このときのＯＫ信号は、ＩＰＳｅｃ処理の一種である認証付暗号ＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｎｇ　Ｓｅｃｕｒｉｔｙ　Ｐｒｏｔｏｃｏｌ）により暗号化されて送信される。

【００４９】ＯＫ信号を受けた鍵転送部１１３は、このＯＫ信号の認証符号を検査し、鍵を転送する相手が本物のゲートウェイＡ２　１２であることを確認する（ステップ２２）。そして、鍵転送部１１３は、鍵転送部１２３に鍵転送を行う（ステップ２３）。

【００５０】このときの鍵データも認証付暗号ＥＳＰによってＩＰＳｅｃ処理される。このような暗号化を行うことによって、ＬＡＮ　Ａ１０内に悪意のユーザが存在しても、盗聴などを行うことはできない。そして、鍵転送部１２３は、送信されてきた鍵データの認証符号を検査し、鍵データを送ったのが本物のゲートウェイＡ１１１であることを確認する（ステップ２４）。

【００５１】最後に、鍵転送部１２３は、転送された鍵を自らの鍵として設定するとともに、鍵転送部１１３に対して、ＯＫ信号を返す（ステップ２５）。このＯＫ信号については、特に認証付暗号ＥＳＰによるＩＰＳｅｃ処理を行う必要はないが、行ってもかまわない。

【００５２】次に、第一実施形態の大規模ＩＰＳｅｃ　ＶＰＮシステムの処理手順について、図４及び図５を参照して説明する。図４は、本実施形態における鍵交換及び鍵転送を説明するためのものであり、図５は、鍵転送が行われた後に、鍵交換を行った大規模ＬＡＮにおけるゲートウェイが故障した場合に、どのようにＩＰＳｅｃ通信が実現されるのかを説明するためのものである。

【００５３】なお、これらの図において、Ｒ１、Ｒ２、Ｒ３は通信回線上に存在し、それぞれゲートウェイＢ　２１、ゲートウェイＡ１　１１、ゲートウェイＡ２　１２との情報の送受信を中継するルータであり、これら以外の構成及びその機能については、図１と同様である。

【００５４】まず、図４において、ゲートウェイＡ１１１とゲートウェイＢ　２１の間で、鍵交換が行われると（ステップ３０）、ゲートウェイＡ１　１１は、ゲートウェイＡ２　１２に対して上述したようなネゴシエー

ションを行って、鍵転送を行う（ステップ３１）。

【００５５】次に、図５において、ゲートウェイＡ１　１１に障害が発生し、通信回線を介した通信が行えなくなると（ステップ４０）、ルーティングプロトコルによってＲ２がこれを認識するとともに、Ｒ１、Ｒ３にその情報を伝達し、ゲートウェイＡ１　１１宛の全てのパケットを、ゲートウェイＡ２　１２に転送するように、経路情報が修正される（ステップ４１）。

【００５６】そして、ＬＡＮ　Ｂ２０におけるホストｂ（Ｈｏｓｔ　ｂ）が、ＬＡＮ　Ａ１０におけるホストａ（Ｈｏｓｔ　ａ）に対してパケットを発信すると（ステップ４２）、ゲートウェイＢ　２１は、このパケットを受け取って、正常時と同様にＩＰＳｅｃのカプセル化を行って（ステップ４３）、最寄りのルータＲ１に転送する。このとき、ステップ４１により転送経路情報が変更されているため、通信回線を通ったパケットは、鍵交換を行ったゲートウェイＡ１　１１ではなく、最終的に、ゲートウェイＡ２　１２にたどり着く（ステップ４４）。

【００５７】ゲートウェイＡ２　１２は、ゲートウェイＢ　２１と共有する鍵をもっているため、これを使って逆カプセル化を行い（ステップ４５）、この逆カプセル化されたパケットは、ゲートウェイＡ２　１２によって、ホストａに転送される（ステップ４６）。このようにして、ゲートウェイＡ１　１１の障害にも拘わらず、ホストａとホストｂ間のＩＰＳｅｃ通信は成立する。

【００５８】［第二実施形態］次に、本発明の第二実施形態につき、図６を参照して説明する。同図は、本実施形態の大規模ＩＰＳｅｃ　ＶＰＮシステムの機能を示すブロック図である。本実施形態は、第一実施形態と比較して、ＬＡＮ　Ａ１０において、鍵転送が複数回行われる点で相違する。

【００５９】同図に示すように、本実施形態の大規模ＩＰＳｅｃ　ＶＰＮシステムのＬＡＮＡ１０は、ゲートウェイＡ１　１１、ゲートウェイＡ２　１２、ゲートウェイＡ３　１３を有している。これ以外の構成及びその機能については、図１におけるものと同様である。まず、ゲートウェイＡ１　１１とゲートウェイＢ　２１間で鍵交換が行われると（ステップ５０）、ゲートウェイＡ１　１１は、この鍵を自らに設定するとともに、ゲートウェイＡ２　１２に対して鍵転送を行う。

【００６０】鍵転送を受けたゲートウェイＡ２　１２は、自ら鍵設定を行うとともに、さらにゲートウェイＡ３　１３に対して、鍵転送を行う。そして、ゲートウェイＡ３　１３は、自ら鍵設定を行うとともに、鍵をさらにゲートウェイＡ１　１１に送信し、ゲートウェイＡ１　１１が、この送信されてきた鍵が、自分が転送した鍵と一致することを確認して鍵転送を終了する（ステップ５１）。

【００６１】なお、本実施形態においては、ＬＡＮ　Ａ１０内の３台のゲートウェイ間で、鍵転送を行っているが、より多くのゲートウェイ間で同様の処理を行うこともできる。また、本実施形態においては、鍵転送を受けたゲートウェイが、次に他のゲートウェイに鍵転送を順次行う手順としているが、より多くのゲートウェイ間で転送処理を行う場合には、所定の鍵転送経路を設定するなどして、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、まだ鍵転送を受けていないゲートウェイに対し、複数の転送を同時に実行することによって、速やかに転送を行うことも可能である。

【００６２】さらに、マルチキャスト（Ｍｕｌｔｉｃａｓｔ）ＩＰＳｅｃによって、大規模ＬＡＮのゲートウェイに一斉に鍵転送し、鍵設定を行うようにしてもよい。また、以上の実施形態では、ＬＡＮ　Ｂ２０内において、鍵転送処理を行ってはいないが、ＬＡＮ　Ｂ２０が複数のゲートウェイを有する場合にはＬＡＮ　Ａ１０における場合と同様に、必要に応じて鍵転送による鍵の共有化を行うことはもちろん可能である。

【００６３】加えて、これらの実施形態におけるゲートウェイの機能を、ＶＰＮ以外に応用することも可能である。すなわち、このような鍵転送機能による鍵の共有化を、例えば、インターネット上にショップを提供するサーバなどの情報処理装置（鍵共有情報処理装置）に用いることにより、インターネットショッピングにおいてセキュリティを確立した後に、一部の情報処理装置に障害が発生したとしても、通信不能となることを防止することが可能となる。

【００６４】そして、このような処理についても、上記実施形態において、ゲートウェイの代わりに鍵共有情報処理装置を用いることにより、同様の構成（ただし、この場合、ＬＡＮ　Ａ１０は大規模でなくともよい。）で、同様の鍵転送プロトコルを用いて実現することが可能である。

【００６５】大規模ＩＰＳｅｃ　ＶＰＮシステムにおける処理手順をこのような順序とすれば、大規模ＬＡＮ内のゲートウェイが鍵をコピーすることによって、実際には鍵交換をしていない相手とも鍵を共有することができるため、複数のゲートウェイを有する大規模なＬＡＮとＩＰＳｅｃによるＶＰＮを構築するにあたり、その一部のゲートウェイの障害などによる通信不能を防止することが可能となる。また、大規模ＬＡＮ内のゲートウェイ間における鍵の共有化を、鍵転送によって行うことにより、このような鍵の共有化を鍵交換によって行う場合に比較すると、装置にかかる負荷を大幅に削減することが可能となる。

【００６６】上記の実施形態における鍵転送等は、大規模ＩＰＳｅｃ　ＶＰＮプログラムにより実行される。この大規模ＩＰＳｅｃ　ＶＰＮプログラムは、コンピュータの各構成要素に指令を送り、所定の処理、例えば、鍵

転送処理等を行わせる。これによって、これらの処理は、大規模ＩＰＳｅｃ　ＶＰＮプログラムとコンピュータとが協働したゲートウェイＡ１　１１、ゲートウェイＡ２　１２等により実現される。

【００６７】なお、大規模ＩＰＳｅｃ　ＶＰＮプログラムは、コンピュータのＲＯＭやハードディスクに記憶させる他、コンピュータ読み取り可能な記録媒体、例えば、外部記憶装置及び可搬記録媒体等に格納することができる。外部記憶装置とは、磁気ディスク等の記録媒体を内蔵し、例えばゲートウェイＡ１　１１などに外部接続される記憶増設装置をいう。一方、可搬記録媒体とは、記録媒体駆動装置（ドライブ装置）に装着でき、かつ、持ち運び可能な記録媒体であって、例えば、ＣＤ－ＲＯＭ、フレキシブルディスク、メモリカード、光磁気ディスク等をいう。

【００６８】そして、記録媒体に記録されたプログラムは、コンピュータのＲＡＭにロードされて、ＣＰＵにより実行される。この実行により、上述した本実施形態のゲートウェイＡ１　１１、ゲートウェイＡ２　１２等の機能が実現される。さらに、コンピュータで大規模ＩＰＳｅｃ　ＶＰＮプログラムをロードする場合、他のコンピュータで保有された大規模ＩＰＳｅｃ　ＶＰＮプログラムを、通信回線を利用して自己の有するＲＡＭや外部記憶装置にダウンロードすることもできる。このダウンロードされた大規模ＩＰＳｅｃ　ＶＰＮプログラムも、ＣＰＵにより実行され、鍵転送処理等を実現する。

【００６９】なお、本発明は以上の実施形態に限定されるものではなく、これをＶＰＮ構築以外の場合にも応用することができる。例えば、インターネットショッピングにおいて、利用者端末が、ショップのサーバとセキュリティを確立する際に、ショップの別個のサーバに鍵転送を行うことによって、利用者のショッピング中にショップのサーバに障害が発生しても、その別個のサーバに以降の処理を代行させることによって、通信不能とならなくするなど、適宜設計変更できるものである。

【００７０】

【発明の効果】以上のように、本発明によれば、複数のゲートウェイを有する大規模なＬＡＮとＩＰＳｅｃによるＶＰＮを構築する場合に、一部のゲートウェイの障害などによる通信不能を防止することができる。

【００７１】また、鍵交換によって装置にかかる負荷を大幅に軽減することが可能となる。すなわち、ＩＫＥによる鍵交換は、公開鍵暗号技術にもとづく処理であり、他の処理に比べて非常に負荷が大きく、障害時の迂回を考えて２つ以上のゲートウェイとそれぞれ鍵交換を行えば、ゲートウェイの台数分だけ鍵交換を行う必要があるが、本方式では１度の鍵交換でよい。

【００７２】さらに、システム全体を安価に構築することが期待できる。これは、パケットがどのゲートウェイに渡されるかはインターネット上のルータが決める方式であるため、大規模なＬＡＮにアクセスする側のＬＡＮは、相手のどのゲートウェイと通信しているかを意識しなくて良いからである。すなわち、これは本方式を実現するためにアクセスする側のゲートウェイに特別な仕掛けが必要ないことを意味する。

【００７３】このようなネットワークは、一般に、１つの大規模ＬＡＮに多数の小規模ＬＡＮがアクセスする構成をとるため、小規模ＬＡＮ側のゲートウェイとして、ＩＰＳｅｃ／ＩＫＥに対応した通常のＩＰＳｅｃ　ゲートウェイを用いることができれば、システム全体として安価なものとなる。

【００７４】また、大規模ＩＰＳｅｃ　ＶＰＮプログラムは、コンピュータの各構成要素へ所定の指令を送ることにより、このコンピュータに、鍵転送機能等を実現させることができる。これによって、これらの機能等は、大規模ＩＰＳｅｃ　ＶＰＮプログラムとコンピュータとが協働したゲートウェイ等により実現可能である。

【図面の簡単な説明】

【図１】本発明の第一実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムの構成を示すブロック図である。

【図２】本発明の第一実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムのゲートウェイの機能を示すブロック図である。

【図３】本発明の各実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムの鍵転送プロトコルの動作を示す動作手順図である。

【図４】本発明の第一実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムの機能を示すブロック図（１）である。

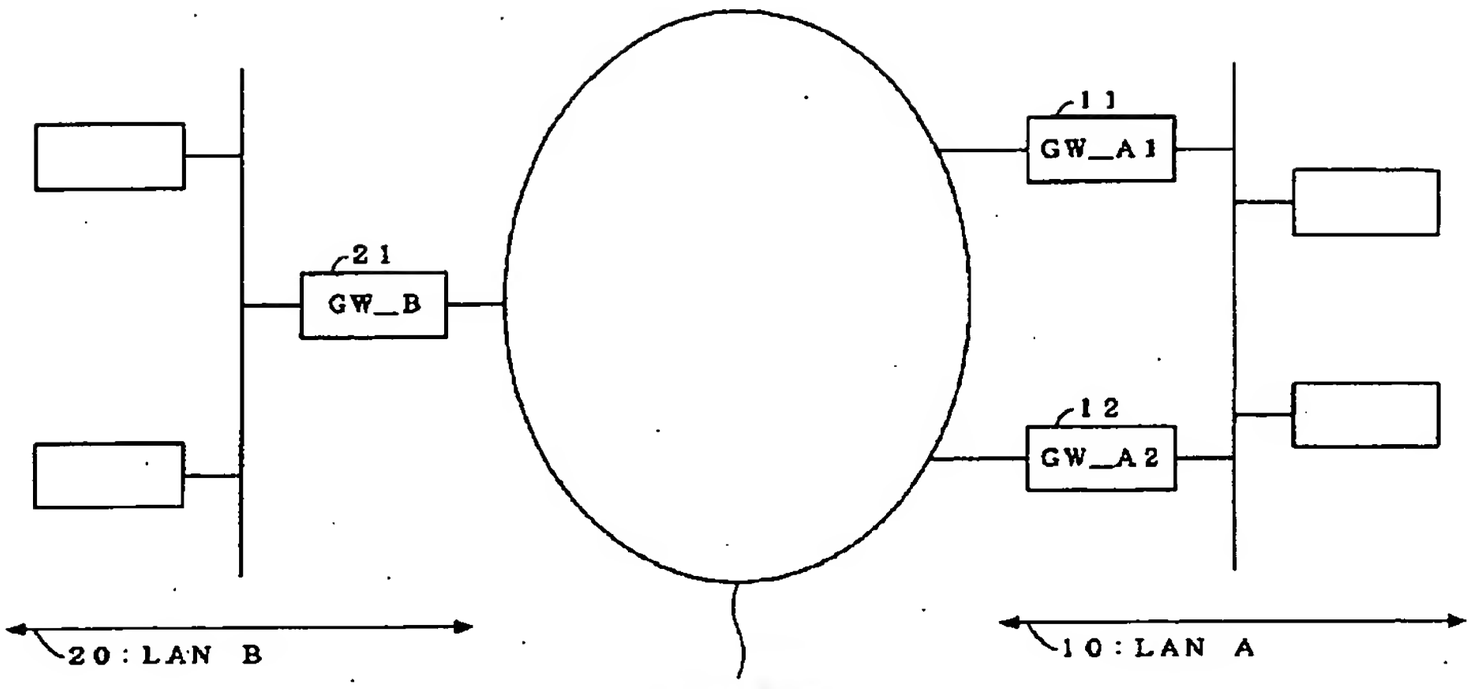
【図５】本発明の第一実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムの機能を示すブロック図（２）である。

【図６】本発明の第二実施形態における大規模ＩＰＳｅｃ　ＶＰＮシステムの機能を示すブロック図である。

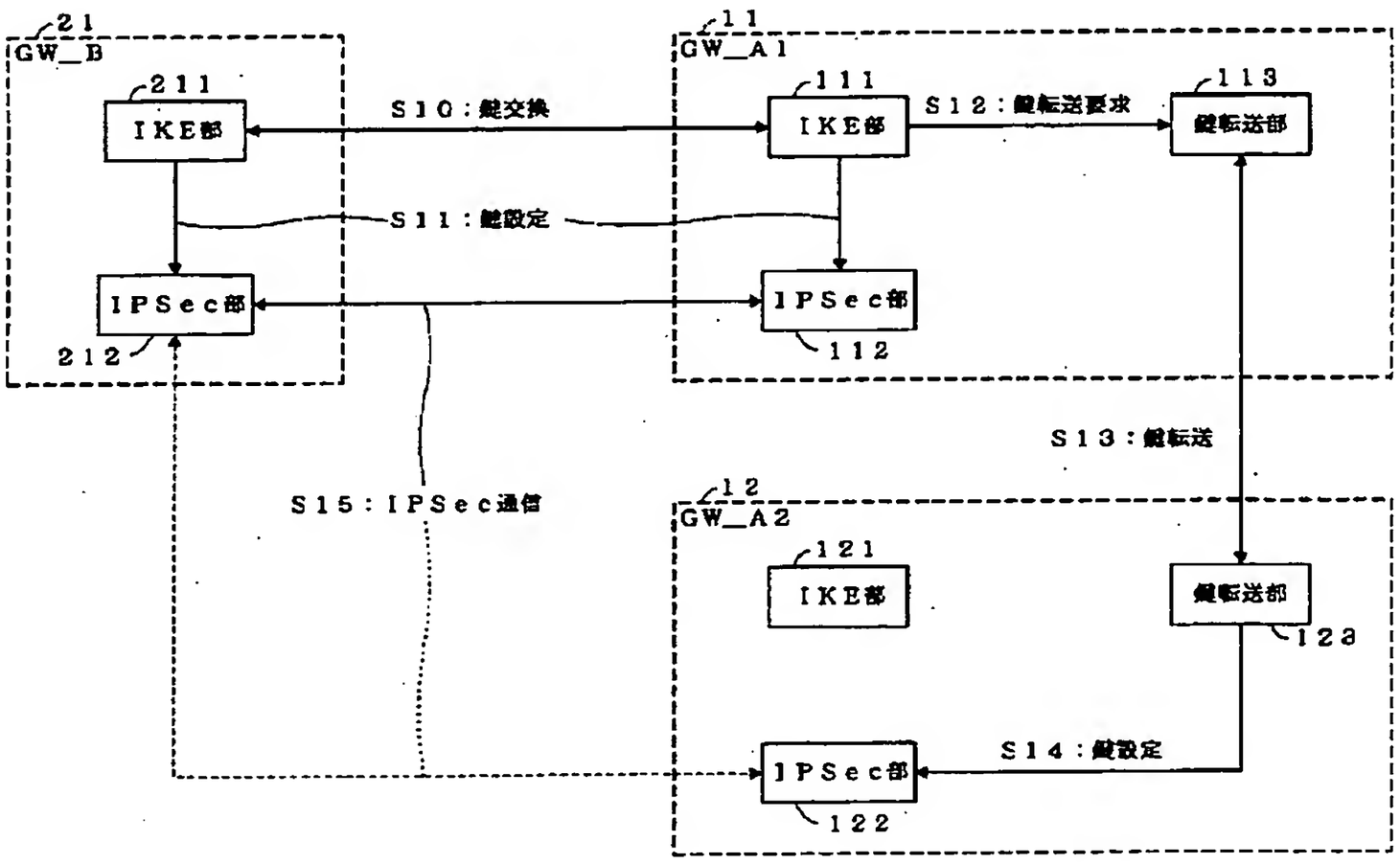
【符号の説明】

１０　ＬＡＮ　Ａ
１１　ゲートウェイＡ１（ＧＷ＿Ａ１）
１２　ゲートウェイＡ２（ＧＷ＿Ａ２）
１３　ゲートウェイＡ３（ＧＷ＿Ａ３）
１４　ホストａ（Ｈｏｓｔ　ａ）
２０　ＬＡＮ　Ｂ
２１　ゲートウェイＢ（ＧＷ＿Ｂ）
２２　ホストｂ（Ｈｏｓｔ　ｂ）
３０　通信回線
３１　ルータ１（Ｒ１）
３２　ルータ２（Ｒ２）
３３　ルータ３（Ｒ３）

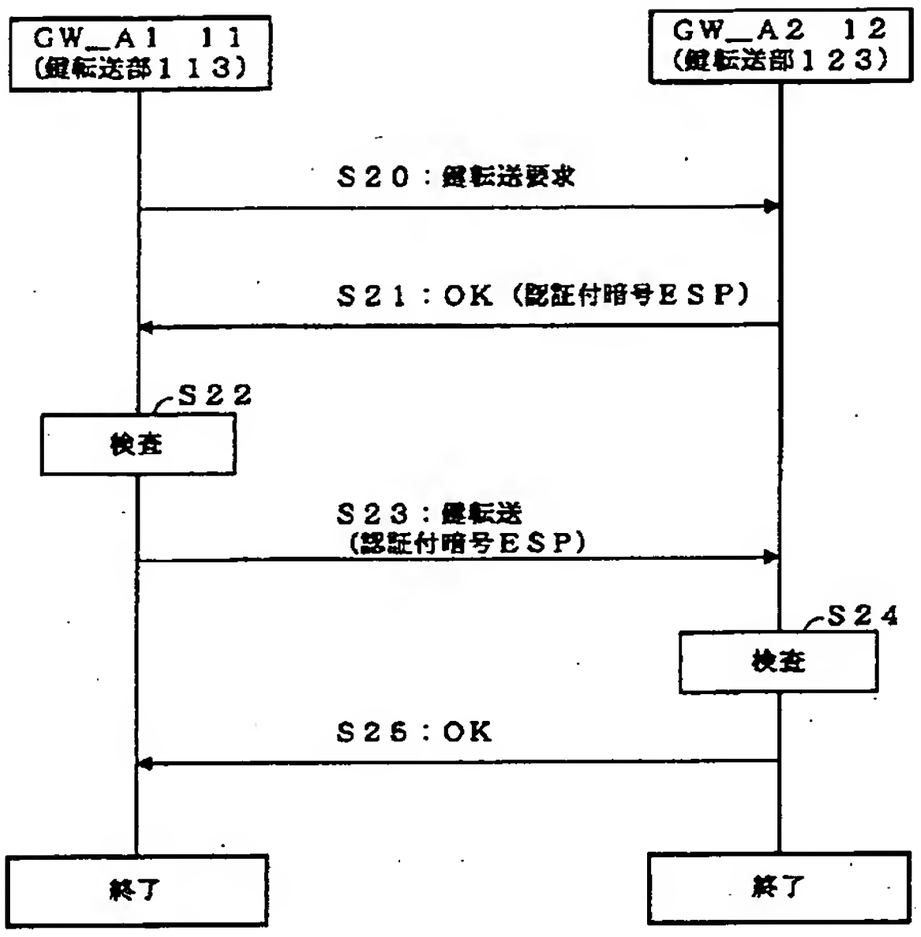
【図１】


11
GW_A1
21
GW_B
12
GW_A2
20：LAN B
10：LAN A
30：通信回線

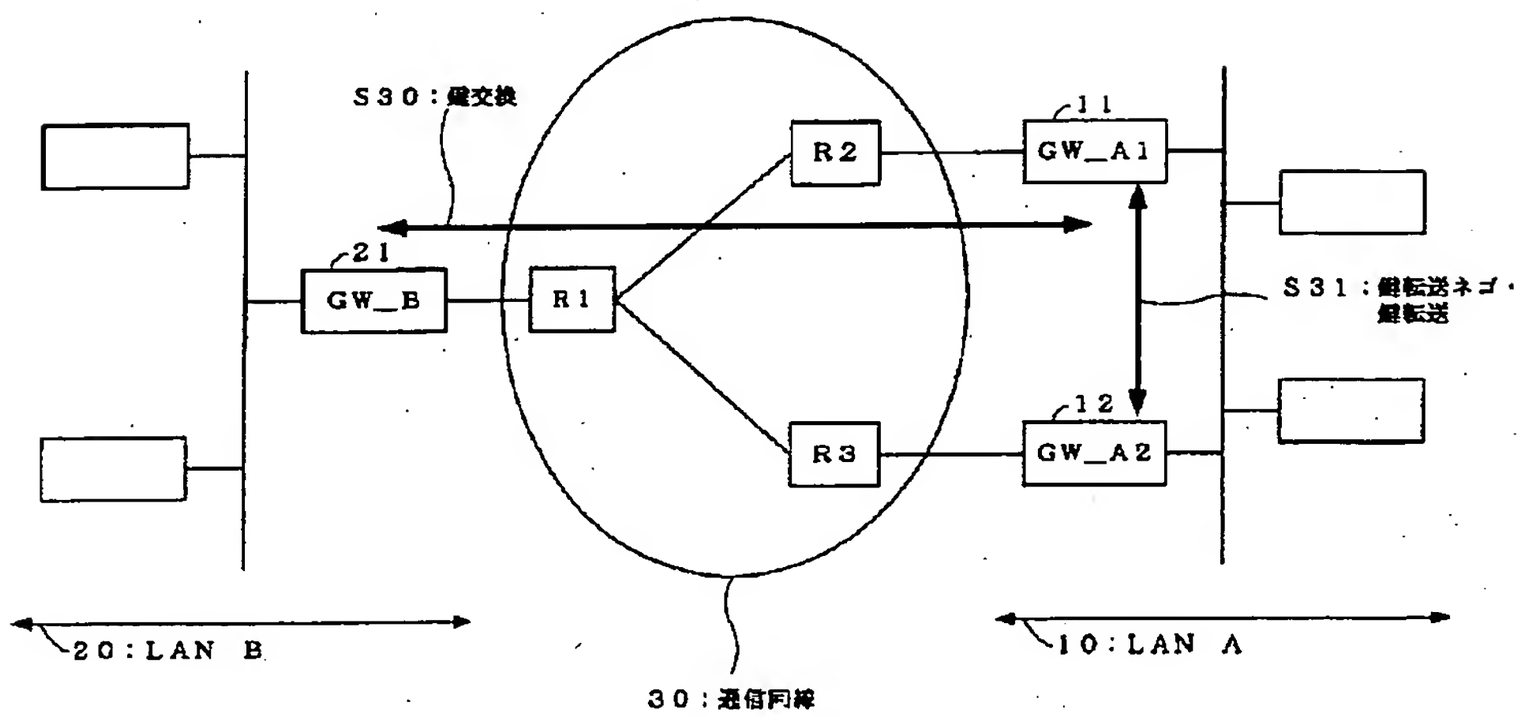
【図２】


21
GW_B
211
IKE部
212
IPSec部
S10：鍵交換
S11：鍵設定
S15：IPSec通信
11
GW_A1
111
IKE部
112
IPSec部
S12：鍵転送要求
113
鍵転送部
S13：鍵転送
12
GW_A2
121
IKE部
122
IPSec部
S14：鍵設定
123
鍵転送部

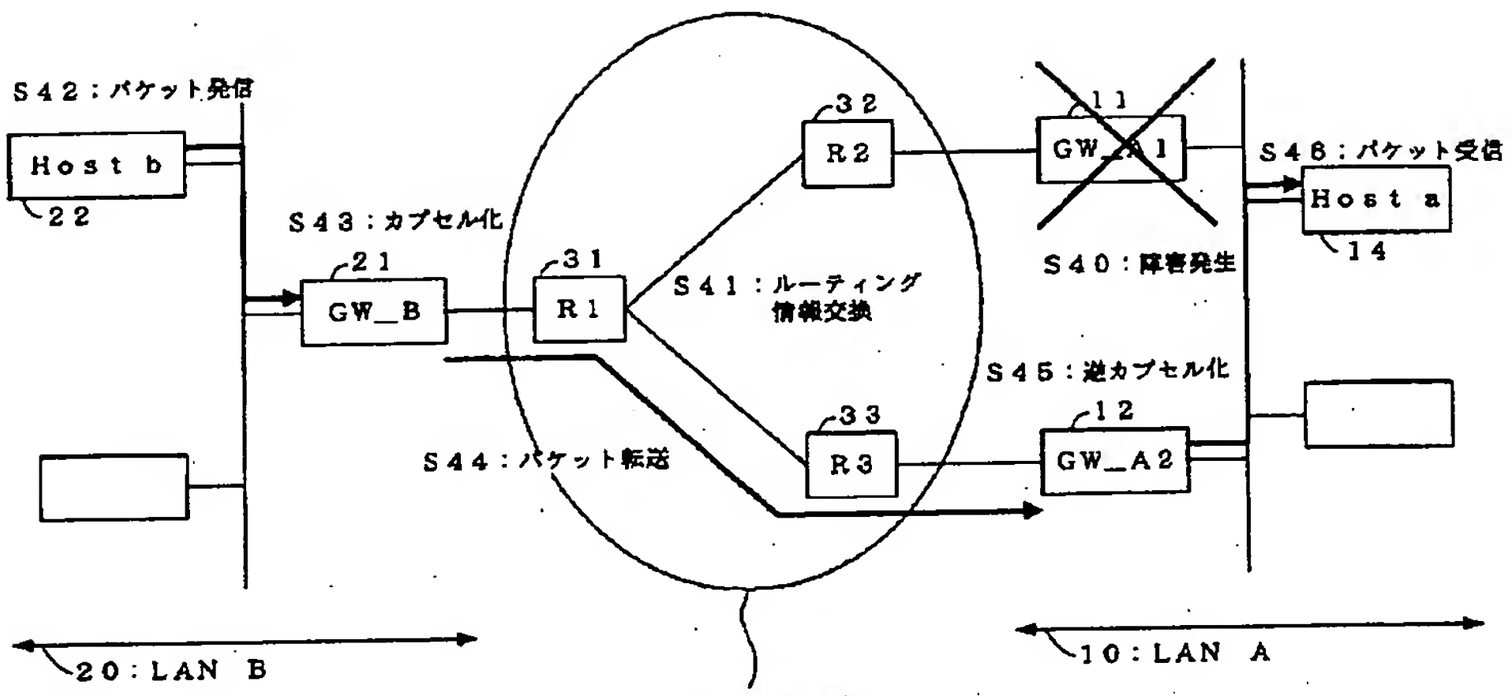
【図３】


GW_A1　11
(鍵転送部113)
GW_A2　12
(鍵転送部123)
S20：鍵転送要求
S21：OK（認証付暗号ESP）
S22
検査
S23：鍵転送
（認証付暗号ESP）
S24
検査
S25：OK
終了
終了

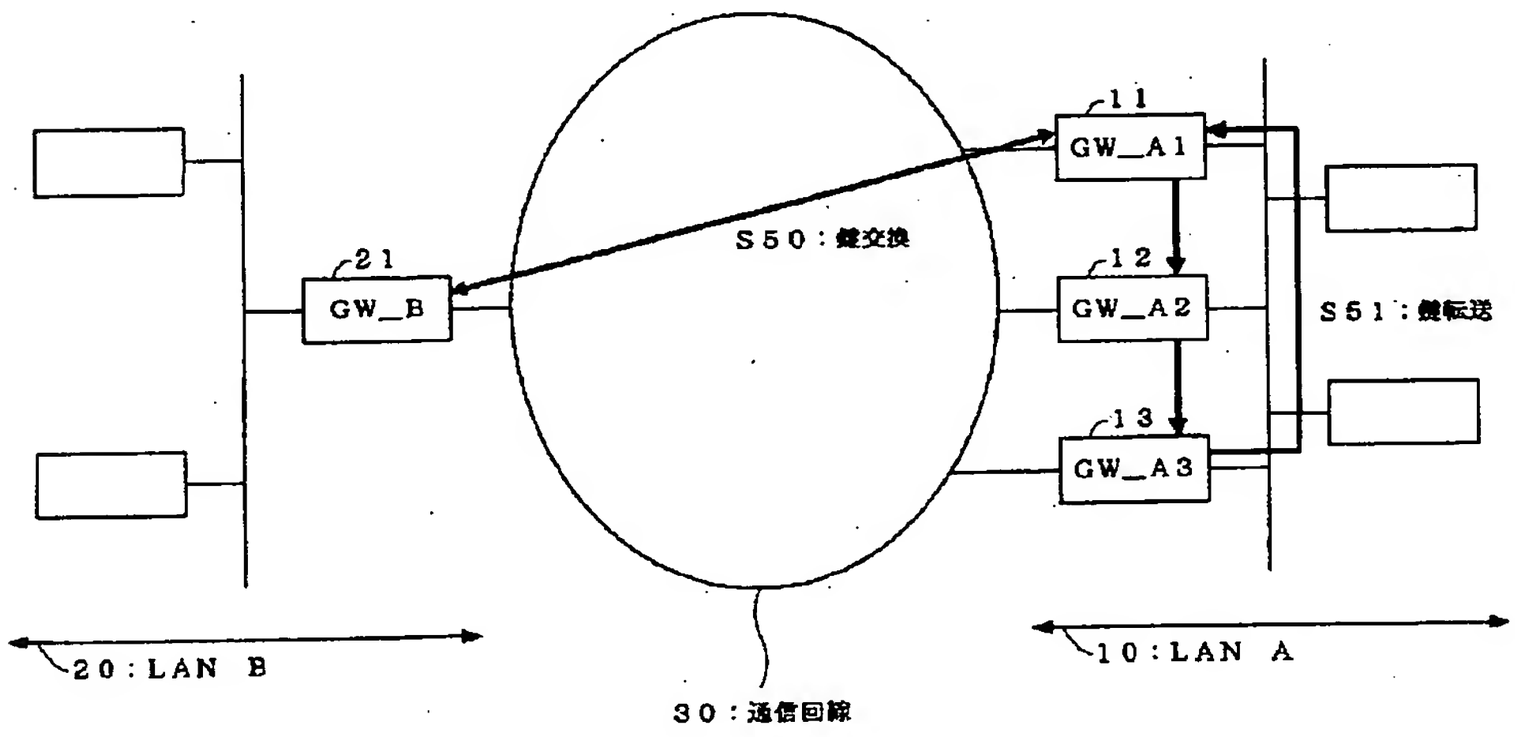
【図４】


S30：鍵交換
11
GW_A1
R2
21
GW_B
R1
R3
12
GW_A2
S31：鍵転送ネゴ・
鍵転送
20：LAN B
10：LAN A
30：通信回線

【図５】


S42：パケット発信
Host b
22
S43：カプセル化
21
GW_B
31
R1
32
R2
S41：ルーティング
情報交換
33
R3
S44：パケット転送
11
GW_A1
S40：障害発生
S46：パケット受信
Host a
14
S45：逆カプセル化
12
GW_A2
20：LAN B
10：LAN A
30：通信回線

【図６】


11
GW_A1
S50：鍵交換
21
GW_B
12
GW_A2
S51：鍵転送
13
GW_A3
20：LAN B
10：LAN A
30：通信回線